REMARKS

Applicant respectfully requests that the above application be reconsidered in view of the above amendments and following remarks. Claims 1-20 are currently pending; Claims 10-20 have been allowed.

A. Response to Rejection of Claims 1-3 and 8-9 under 35 USC 102(b) as Anticipated by Howard et al

At pages 2-3 of the Office Action (see paragraph 1), the Examiner has rejected Claims 1-3 and 8-9 under 35 USC 102(b) as anticipated by U.S. Patent 6,442,690 (Howard et al):

Claim 1: Howard's patent discloses remote device control method where in response to the request (fig. 14), generating a challenge that includes what operation to be performed on the host computer was requested in (fig. 14) note that device signs the message in response to IKMS request. Further, certificate contains a message that includes types of operations such as device initialization, network operations, rekeying (col. 23, lines 56-58; col. 21, lines 64-67). Encrypting the challenge is disclosed by Howard in (fig. 14). Howard discloses transmitting the encrypted challenge to a secure environment that contains the client user's private key in (col. 26, lines 34-35). Howard discloses decrypting the challenge in the secure environment and securely displaying the decrypted challenge in (col. 26, lines 39-40). Howard discloses confirmation where user transmits a reply encrypted with the host computer's public key to the host computer that contains a positive response and the nonce in (fig. 14, K3). Note transmission of acknowledgement and message signing.

Claim 2: Howard discloses request is for access to a resource on the host computer in (col. 27, lines 25-40).

Claim 3: Howard discloses challenge encrypted during step (2) is encrypted with the user's public key in (col. 28, lines 46-62).

Claims 8-9: Howard discloses confirmation in (fig. 14).

Applicant respectfully traverses this rejection. Contrary to what the Examiner suggests, Howard et al does not disclose the following in the method of Claims 1-3 and 8-9: (1) in response to the request to perform the operation on the host computer, generating a challenge that

includes what operation was requested, a nonce and a query as to whether the client user made this request; (2) after decrypting the challenge, securely displaying the encrypted challenge; and (3) waiting for confirmation from the client user that securely confirms whether or not the client user made the request to perform the operation. See Claim 1 (steps 1, 4 and 5) (emphasis added).

Unlike the method of Claims 1-3 and 8-9, Howard et al does not show a challenge to confirm what operation is to be performed. Instead, this reference shows purely a request to replace an existing certificate with a new one (K2) and an acknowledgement that the replacement occurred (K3). There is no confirmation in the Howard et al system of the user's intent to perform the operation as in Applicant's claimed method.

In addition, and contrary to what the Examiner suggests, Howard et al does not teach transmitting encrypted challenge to a secure environment that contains the user's private key. What Howard et al discloses is not a "challenge" but instead a new public-private key pair, i.e., a new set of encryption keys. Also, contrary to what the Examiner suggests, Howard et al does not teach securely displaying a decrypted challenge to the user (e.g., human). Moreover, in the Howard et al system, the acknowledgement is the acknowledgement from the device that it received a new set of encryption keys for the IKMS. By contrast, in the method of Claims 1-3 and 8-9, there is an acknowledgement/confirmation that a client user intended to make a particular request.

Regarding the Examiner's comments on Claim 3, Howard et al does disclose that the challenge is encrypted with the user's public key. However, contrary to what the Examiner suggests and for reasons previously given , the challenge encrypted according to Claim 3 is different from that of Howard et al.

Regarding the Examiner's comments on Claims 8-9, there is no user confirmation or prompt for confirmation from a user (human) in Fig 14 of Howard et al, i.e., confirmation that that a task was performed (changed keys). By contrast, in the method of Claims 8-9, there is confirmation: (a) by a user (person); and (b) an indication of whether this person intended to access a resource on the host computer.

For these reasons, Applicant submits that Claims 1-3 and 8-9 are novel and unobvious over Howard et al.

B. Response to Rejection of Claims 4-6 under 35 USC 103(a) as obvious over Howard et al in view of Caputo et al

At page 3 of the Office Action (see paragraph 2), the Examiner Claims 4-6 have been rejected by the Examiner as unpatentable (i.e. obvious) over Howard et al, in view of U.S. Patent 5,546,463 (Caputo et al):

Howard does not specifically disclose intelligent token containing user's private key that is capable of decrypting the encrypted challenge. Caputo discloses intelligent token containing user's private key that is capable of decrypting the encrypted challenge in (fig. 5A, 6). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ intelligent token as taught in Caputo with system disclosed in Howard in order to protect keys from hijackers. Since key is stored in a portable storage and not in the fixed terminal, user can transport keys from device to device where key attacks and tampering can be minimized.

Applicant respectfully traverses this rejection for reasons previously presented as to why the method of Claims 1-3 and 8-9 are novel and unobvious over Howard et al. What is taught by Caputo et al does not change the fundamental fact that the primary fact that the primary reference, Howard et al, fails to teach the basic method of Claims 4-6. The method of Claim 5 is further distinguishable in that it includes a secure display unit (e.g. a smart card reader with a display screen or area) to display a decrypted challenge with the ability to display the decrypted challenge without it having possibly been modified (even if the client workstation is compromised by something such as a virus). The method of Claim 6 is further distinguishable in that that the secure display unit is able to display the challenge without the possibility that the challenge could be altered, for example, by an attacker/virus, even if the attacker/virus has compromised the client computer).

For the foregoing reasons, Applicant submits that Claims 4-6 are unobvious over Howard et al, even in view of Caputo et al.

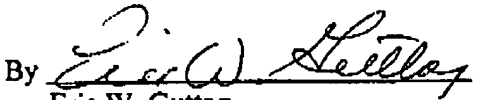
C. Response to Objection to Claim 7

At page 4 of the Office Action, the Examiner has objected to Claim 7 as being depending upon a rejected base claim, but says it would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claim. Applicant agrees with the Examiner's determination that the method of Claim 7 is not taught by the art of record. However, Applicant submits that that, for reasons presented previously, that Claim 1 that Claim 7 ultimately depends from is also allowable. Accordingly, Applicant respectfully requests that the Examiner withdraw his objection to Claim 7.

D. Conclusion

Applicant submits that Claims 1-20are novel and unobvious over the art relied on by the Examiner. Accordingly, Applicant requests that the above application be allowed to issue with Claims 1-20 currently pending.

Respectfully submitted,
For: Neil R. FRASER

By 
Eric W. Guttag
Attorney for Applicant
Registration No. 28,853
(513) 229-0383
Customer No. 26868

June 14, 2004
Mason, Ohio